Menghadapi Serangan Digital

Setiap jurnalis harus tetap mewaspadai setiap bentuk-bentuk serangan digital. Pengetahuan berupa langkah-langkah darurat yang harus dilakukan saat serangan terjadi harus dimiliki oleh jurnalis. Selain mengetahui langkah-langkah teknis di bawah ini, melapor ke perusahaan media tempat Anda bekerja dan ke pengurus AJI Kota adalah hal yang penting dilakukan untuk meminta dukungan dan bantuan darurat. Untuk Pengurus AJI Kota, harus memantau kondisi korban, membantu mencari rumah aman, dan mengadvokasi kasus apabila skala serangan meluas dan mengancam nyawa.

1. **Peretasan Yahoo Mail**
   a. Reset password Anda dengan masuk ke halaman ini: https://s.id/ResetYahoo
   b. Masukkan alamat email akun Yahoo Mail Anda
   c. Pilih metode reset yang diinginkan, melalui nomor HP atau email pemulihan yang sudah Anda daftarkan. Namun pemulihan melalui email lebih direkomendasikan. Klik Next.
   d. Sebuah kode akan dikirimkan ke email pemulihan atau via SMS. Masukkan kode itu ke halaman Yahoo.
   e. Buat password baru yang lebih kuat dengan kombinasi angka, huruf dan spasi.

2. **Peretasan Gmail**
   a. Apabila Anda masih bisa mengakses akun Gmail Anda, segera ubah password dan tambahkan autentifikasi 2 langkah (bagi yang belum mengaktifkan).
   b. Apabila Anda tidak bisa login, buka halaman pemulihan akun dengan klik tautan ini: https://s.id/PemulihanGmail. Jawab pertanyaan-pertanyaan yang diajukan oleh Google. Jika dimintai sandi terakhir yang Anda ingat, masukkan sandi paling baru yang diingat. Semakin terbaru sandinya, akan semakin baik. Masukkan alamat email pemulihan yang dapat membantu Anda untuk kembali login dan menjadi email tujuan pengiriman pemberitahuan keamanan.
   c. Selengkapnya mengenai peretasan dan pemulihan akun Gmail, bisa mengikuti langkah-langkah dalam tautan ini: https://s.id/LoginGmail

3. **Peretasan akun Whatsapp:**
   a. Uninstall WA ponsel Anda lalu Install kembali
   b. Daftarkan nomor Anda dan tunggu kode verifikasi melalui SMS
   c. Masukkan segera kode verifikasi 6 digit dari SMS
   d. Jika Anda tidak menerima kode 6 digit melalui SMS, tunggu hingga bilah kemajuan selesai dan coba lagi. Waktu tunggu dapat berlangsung hingga 10 menit.
   e. Jika waktu timer berakhir sebelum Anda menerima kode verifikasi, sebuah opsi akan muncul untuk meminta panggilan telepon. Pilih opsi "*Panggil saya*" untuk meminta panggilan telepon. Ketika Anda menerima panggilan, mesin suara otomatis akan memberitahu Anda kode verifikasi 6 digit. Masukkan kode ini untuk memverifikasi akun WhatsApp Anda.
   f. Saat akun Anda, segera tambahkan PIN dan email agar akun Whatsapp Anda tidak dicuri kembali.

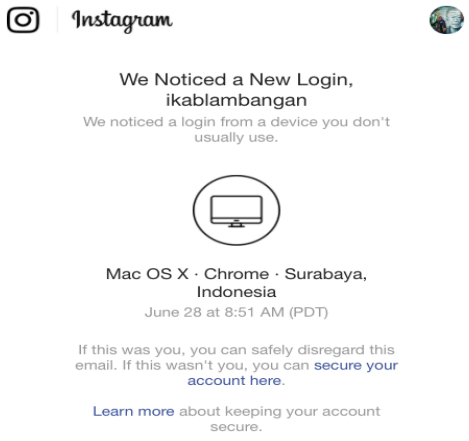
g. Apabila Anda masih sulit masuk dan diminta untuk memasukkan kode verifikasi dua langkah, peretas mungkin telah mengaktifkan PIN. Anda harus menunggu selama 7 hari sebelum dapat masuk ke akun tanpa kode verifikasi dua langkah.
h. Laporkan bahwa akun Anda telah dicuri ke: *support@whatsapp.com* dengan subyek '*Hilang / Dicuri: Silakan nonaktifkan akun saya*' di badan email.

2. Peretasan Akun Facebook

a. Untuk mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam, Anda bisa memeriksa di *Pengaturan* ⇒ *Keamanan dan Info Login*. Lalu periksa "*Tempat Anda Login*" untuk mengecek daftar perangkat (laptop atau ponsel) yang mengakses akun Anda. Apabila menemukan perangkat yang bukan milik Anda, klik *tiga titik* di sebelah kanan, lalu pilih keluar. Anda juga perlu mengganti password yang lebih kuat.
b. Saat akun Anda telah diretas dan password diubah, Facebook akan mengirimkan notifikasi melalui email yang Anda daftarkan. Cek notifikasi tersebut!
c. Dalam email notifikasi, Facebook menyediakan tautan *"Klik di sini"* untuk Anda yang tidak membuat perubahan password tersebut.
d. Tautan itu akan mengarahkan Anda untuk menjawab pertanyaan yang diminta oleh Facebook untuk memulihkan akun Anda.
e. Atau Anda bisa mengakses tautan berikut untuk melaporkan peretasan yang terjadi: https://www.facebook.com/hacked

3. Peretasan Akun Instagram

a. Apabila Anda menggunakan laptop, Anda bisa mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam, dengan memeriksa di *Pengaturan* ⇒ *Login activity*. Anda akan dibawa pada sebuah halaman yang berisi informasi tentang jenis perangkat dan lokasi login. Apabila Anda menemukan adanya perangkat yang tidak Anda gunakan, klik tanda panah di sebelah kanan, lalu klik *logout*.
b. Apabila Anda sudah tidak bisa masuk ke akun Instagram, cek pemberitahuan (notice) di alamat email yang Anda daftarkan. Instagram akan mengirimkan pemberitahuan pada setiap perubahan yang terjadi pada akun Instagram Anda, seperti login dari perangkat berbeda atau perubahan password. Berikut contohnya:



c. Klik *Secure Your Account Here* dan Anda akan dibawa pada halaman untuk mengubah *password* Instagram Anda. Segera masukkan password baru yang lebih kuat dan unik.
d. Apabila Anda tetap kesulitan mengambil-alih akun, laporkan ke Instagram dengan langkah-langkah:

   Di Android:

   - Di layar login, ketuk *Dapatkan bantuan untuk login* di bawah *Login*.
   - Masukkan nama pengguna, email, atau nomor telepon Anda, lalu ketuk *Berikutnya*. Pelajari selengkapnya tentang apa yang bisa Anda lakukan jika tidak tahu nama pengguna Anda.
   - *Ketuk Perlu bantuan lain*?, lalu ikuti petunjuk di layar.
   - Pastikan Anda memasukkan alamat email yang aman dan hanya bisa diakses oleh Anda. Setelah mengirimkan permintaan, tunggu email dari Instagram yang berisi langkah berikutnya.

   Di iOS:

   - Di layar *login*, ketuk *Lupa kata sandi?*
   - Ketuk *Perlu bantuan lain*? di bawah tombol *Berikutnya* dan ikuti petunjuk di layar.
   - Pastikan Anda memasukkan alamat email yang aman dan hanya bisa diakses oleh Anda. Setelah mengirimkan permintaan, tunggu email dari Instagram yang berisi langkah berikutnya.
e. Baca selengkapnya terkait pemulihan akun yang diretas di: *https://help.instagram.com/* ⇒ *Pusat Privasi dan Keselamatan* ⇒ *Melaporkan Sesuatu* ⇒ *Akun yang Dibajak*.

4. Peretasan Akun Twitter

a. Apabila Anda tidak bisa login, atur ulang kata sandi Anda dengan meminta email dari: *https://twitter.com/account/begin_password_reset*
b. Coba masukkan nama pengguna dan alamat email Anda, dan pastikan untuk memeriksa email pengaturan ulang di alamat email yang Anda daftarkan untuk akun Twitter Anda.
c. Jika Anda telah berhasil masuk kembali, silakan atur ulang keamanan akun Anda dengan meninjau penggunaan verifikasi dua langkah.
d. Jika Anda tetap tidak bisa masuk, hubungi Twitter dengan membuka halaman di: *https://help.twitter.com/forms* lalu pilih *Akun yang diretas* dari daftar pilihan. Pastikan untuk menggunakan alamat email yang Anda kaitkan dengan akun Twitter yang diretas. Twitter akan mengirimkan informasi dan instruksi tambahan ke alamat email tersebut. Sertakan nama pengguna dan tanggal terakhir Anda mengakses akun.

5. Peretasan Akun Gojek/Grab

a. Uninstall akun Gojek/Grab Anda untuk sementara waktu

b. Lalu hubungi dan jelaskan kronologi kasus Anda ke customer service Gojek di 021-5084-9000 or via e-mail to customerservice@gojek.com. Untuk customer service Grab hubungi 021-50816600.
c. Untuk memulihkan akun Anda, Gojek/Grab biasanya akan meminta untuk menginstal dan memasukkan akun Anda kembali.

6. Menghadapi Doxing

a. Jika doxxer mengungkap alamat rumah Anda dan berpotensi membahayakan keselamatan Anda dan keluarga, pertimbangkan untuk mengungsi ke tempat yang dianggap lebih aman untuk sementara waktu hingga serangan mereda.
b. Laporkan postingan yang mengandung doxing ke platform dan blokir akun pelaku doxxer. Fitur *report* tersedia di masing-masing platform.
c. Jika doxxer mengungkap nomor telepon dan Anda menerima banyak gangguan, matikan telepon Anda sementara waktu. Pertimbangkan untuk mengganti nomor telepon di kemudian hari.
d. Jika doxxer telah mengekspos bank, kartu kredit, atau informasi akun keuangan Anda lainnya, segera hubungi semua lembaga keuangan yang terlibat dan laporkan pelanggarannya.
e. Menutup sementara akun media sosial menjadi pilihan terbaik jika serangan doxxer meningkat.
f. Laporkan ke polisi atas doxing yang Anda alami dengan membawa hasil dokumentasi dan urlnya.

7. Menghadapi Impersonating/pemalsuan akun

1. Buat pengumuman atas pemalsuan akun Anda ke keluarga, rekan kerja dan teman-teman Anda agar mereka tidak tertipu.
2. Laporkan akun yang menggunakan identitas Anda ke penyedia platform agar akun palsu tersebut ditutup.
   Pelaporan akun palsu di FB: https://s.id/akunpalsuFB
   Pelaporan akun palsu di Twitter: https://help.twitter.com/forms/impersonation
   Pelaporan akun palsu di Instagram: https://s.id/akunpalsuIG
   Pelaporan akun palsu Gmail: https://s.id/akunpalsuGmail

8. Menghadapi Pelecehan Online dan KGBO

a. Laporkan/blokir akun, postingan atau komentar yang mengandung pelecehan termasuk KBGO ke platform. Per Januari 2020, Facebook dan Instagram telah memperluas jenis laporannya untuk pelecehan seksual, kekerasan dan hate speech yang mengandung SARA.
b. Minta dukungan dari organisasi yang menyediakan layanan pendamping pelecehan/kekerasan seksual.
c. Laporkan ke polisi atas kekerasan dan pelecehan yang Anda terima, baik melalui telepon, sms, chat, atau di media sosial lainnya dengan menyertakan dokumentasi atas kekerasan/pelecehan yang dialami.
d. Minta dukungan perusahaan media atau AJI untuk memfasilitasi layanan pemulihan trauma.